

DECLASSIFIED
Authority E.O. 13526
By SP NARA Date 10/4/11

A26E
Copy 4

~~TOP SECRET~~ ~~U~~

-1-

TICOM/I-191

HOMEWORK OF DR. WILHELM GERLICH ON
RUSSIAN SYSTEMS

The attached homework by Dr. Wilhelm GERLICH of the German Army Sigint Service (NAAST. 1) was written in November, 1945 at the request of TICOM and received from H.Q., A.S.A., Europe under reference ASA-10/ETC/1ab, dated 17th January, 1946. It describes his work on Russian systems in the cryptanalytic section of NAAST 1.

2. The preliminary interrogation report was issued as TICOM/I-156.

TICOM

5th March, 1946.

No. of pages: 12.

copy no. 16

DISTRIBUTION

British:

- 1. D.D.3.
- 2. H.C.G.
- 3. D.D. (M.W.)
- 4. D.D. (A.S.)
- 5. C.C.R.
- 6. Cdr. Tandy
- 7. Major Morgan

U.S.

- 8-11. Op-20-G (4) (via Cdr. Manson)
- 12. G-2 (via Lt. Col. Hilles)
- 13-16. A.S.A. (4) (via Capt. Collins)
- 17. Director, A.S.A. Europe
- 18. Col. Kuikel, USAAFE

TICOM

- 19-21. S.A.C. (3)
- 22. Cdr. Manson
- 23. Capt. Collins
- 24-27. Ticom Files (4)

Additional

- 28-30. Mr. Pritchard (3)

Do NOT Destroy Return to the
 NSA Technical Library when no longer needed
 S-4851
 I Jan 11 1946

Declassified by D. Janosek,
 Deputy Associate Director for Policy and Records
 on 12/10/2010 and by df

DECLASSIFIED
 Authority E.O. 13526
 By [Signature] NARA Date 10/4/11

TOP SECRET "SI"

-2-

TICOM/I-191

Experience in Cryptanalytic Section of NAASST 1

By Dr. Wilhelm Gerlich

2/F systems

These were used by subordinate units of the Red Army up to the last stages of the war, but not to the same extent as in the early years. They could always be decyphered if sufficient text was available. Usually only a few lines were sufficient to find the key, particularly in the case of letter text. The P. T. 39 (ПЕРЕКОВОРНАЯ ТАБЛИЦА = word table 1939) can be taken as a fundamental system. Letters and phrases were inserted in a certain order in a 10 x 10 square:

	1	2	3	4	5	6	7	8	9	0
1	0		А		К		Ф	Я		
2	1		Б		Л		Х	(,)		
3	2		В		М		Ц	(-)	читай-те слова	
4	3		Г		Н		Ч	(")		
5	4		Д		О		Ш	(?)		
6	5		Е		Щ		Щ	(!)		
7	6	читай-те буквы	Ж		Р		Ы	(.)		
8	7		З		С		Ь			
9	8		И		Т		Э			
0	9		Й		У		Ю			

Declassified by D. Janosek,
 Deputy Associate Director for Policy and Records
 on 12/10/2010 and by [Signature]

DECLASSIFIED

Authority E.O. 13526
 By SP NARA Date 10/4/11

TOP SECRET "U"

-3-

TICOM/I-191

The characteristic feature of the PT 39 was that the letters had only one equivalent and were arranged in three columns. The remaining squares were filled by words such as "radiogramma (wireless message)" etc. To ascertain whether letters or words were to be sent, the two indicators " ЧИТАЙТЕ БУКВЫ (read letters)" and " ЧИТАЙТЕ СЛОВА (read words)" were required. Thus letter texts could in this table only begin with three different B positions of the cypher elements. The element in front of this had to be " ЧИТАЙТЕ БУКВЫ ", the element following these groups " ЧИТАЙТЕ СЛОВА ". Whatever the recypherment might be the same letters would always occur in the same row and column. E.g. А-К-Ф-Я were always in the same line.

Example:

....	72,	65	55	25	55	73	93	95	63	55	23	85	95
	ЧИТАЙТЕ	П	О	Л	О	Ж	И	Т	Е	О	Б	С	Т
	БУКВЫ												
13	45	55	33	15	05								
А	Н	О	В	К	У								

= "Report position".

Method of solution: 1) find the indicators.
 2) find frequency of each cypher element and structure of letter text.

The frequency of each letter had been ascertained from a large number of clear texts, and a long text corresponded with this. In the case of shorter texts the frequency peaks were often considerably displaced, so that one had only the word structure as starting point of attack.

The PT 39 was no longer used in the latter years. About 1941 the Russians introduced other word tables and these could always be reconstructed as far as the letters were concerned. Reconstruction of the arrangement of words was very difficult and success was limited.

Practically all the new word tables of the Red Army had more than one equivalent for each letter. The first to appear were 4 - 6 new word tables, e.g. PT 456 etc.; however I can no longer remember them.

DECLASSIFIED
 Authority E.O. 13526
 By SP8 NARA Date 10/4/11

TOP SECRET "U"

-4-

TICOM/L-191

	1	2	3	4	5	6	7	8	9	∅
1	Ф	А	П	∅	Я	Й	2	В	6	Е
2	О	Х	Ч	Э	Б	6	Р	3	Ц	Ш
3	9	∅	Г	И	8	2	0	5	1	И
4	И	(.)	Ш	8	Р	В	У	7	А	Ы
5	П	Ю	Б	А	Ф	О	Е	Б	Н	Ч. Б.
6	Н	В	Я	9	С	7	Г	Ю	3	Р
7	Ш	Й	Ж	О	К	Ч. С.	К	Е	Ы	(,)
8	К	Б	У	3	Ч	Д	1	Н	5	Л
9	Т	Ч	И	Ж	(,)	Э	К	(.)	Д	3
∅	Е	П	Ц	Л	3	4	Ш	Ю	Л	М

Such a table is given as an example. This use of several equivalents completely obscured the frequency peaks, considerably increasing the difficulty of breaking. As however the Russian encyphers had difficulty in finding the letters, they very often used the same square habitually, and thus we were able as a result of their laziness to discern structure and frequency. New cyphers which were solved were sent (for recognition) as "new cyphers" to the General of Sigint for passing on to the Sigint stations of the other army groups; they automatically sent us cyphers solved or partly solved by other sigint stations.

We possessed about 500 solved 2/F cyphers, of which one or another was always appearing. But as already mentioned, almost all 2/F systems

could be solved and presented no appreciable difficulty to the cryptanalyst.

One or two men were sufficient at Sigint Station 1 to cope with current decyphering of 2/F messages, especially as the greater part of them were already being solved in the companies. Solution was made easier when P/L was interspersed. This also applies to all systems and was constantly occurring.

In the last stages 2/F systems only occurred where the units were engaged in fighting; thus it is to be expected that they are still being used in the Red Army even if they are not appearing at the moment.

The 3/F System.

This is a further development as compared with the 2/F system. Here 1000 cypher elements are available, whereas in the 2/F system there are only 100. Either up to 1000 words may be inserted, or else 2 - 3 or even more figure groups may be used for each P/L element, i.e. more than one equivalent. For instance, in a small code of 5 pages the pages might be numbered as follows:

Page	1	2	3	4	5	
I	2/4	6/7	1/3	5/0	9/8) Encypher- ments.
II	7/4	6/3	1/9	8/2	0/5	

Thus, when reading off one cypher element the page number is taken as position 4 of

the cypher element; as two figures are available for each page (e.g. for encyphering I 2/4 - 6/7 - 1/3 - 5/0 - 9/8), each P/L element may be expressed by 2 cypher elements. Each page is divided into lines, which

DECLASSIFIED

Authority E.O. 13526
 By SP8 NARA Date 10/4/11

TOP SECRET "U"

-5-

TICOM/I-191

again are numbered and from them the DC-positions are read. For these a strip which may be changed is fixed at the edge of each page bearing the figures from 00 to 99. Thus 100 lines may be numbered by it. As however the Russian 3/F codes never have so many word equivalents as to require all the figures the use of more than one equivalent is possible in this case also. Such a strip will accordingly then have a number of consecutive figures for each page of the code, each group forming a so-called "block" [Band]; thus we also speak of "block" equivalents. If now each page has 25 lines, the blocks may be 4 figures long ($100/4 = 25$), so that by means of the blocks alone each word may be expressed by 4 different DC positions. In addition to this there are the double equivalents on each page, so eight cypher equivalents are available for each word. A marginal strip of this type in blocks of 4 figures each would then appear something like this:-

02-06	
98-01	
11-14	
07-10	
23-26	
43-46	
31-34	
51-54	
15-18	APMНЯ/15
39-42	
27-30	
47-50	
19-22	
35-38	

These strips may be exchanged and thus the encypherment changed. Similarly the page numbering may be altered.

Thus after the indicator "read words" the following cypher elements could all stand for the word АРМНЯ (army), if page 1 has the numbering 2/4:

215-216-217-218-415-416-417-418.

If however these groups followed the indicator "read letters" they would mean "A" and after the indicator "read figures" they mean "15".

The codes are usually arranged in "partially alphabetic" order, i.e. alphabetical order is retained, within each letter group, but the letters themselves are not in alphabetical order e.g. K....C....П....A....И.... B etc. As already mentioned the initial letters of the words are used for letter text, single letters not being allotted positions. The figures are dotted about in the text groups.

If we wish to investigate how messages encyphered in this way may be broken, we must begin with the preliminary work necessary.

First of all material which is suspected to be on the same cypher [Verschlüsselung] and which must be of considerable amount, is collected together. Statistics are then made of this material on a large 10 x 10 square. We pay attention to the predominance of cypher elements in certain squares, and to the various frequencies and by these means can weed out messages which probably do not belong to this recypherment [Überschlüsselung].

In the light of these statistics we now examine the messages, and compare the manner in which common cypher elements occur in the messages and in what positions. In this way repeats are ascertained. However, we must compare not only identical figures but also similar ones as we wish first of all to reconstruct the key strip blocks. Here the carelessness of the encypherer is of assistance, for he does not use the whole block but more frequently the first and last figures of it, as they have been entered direct in the key. When the bands have been ascertained

DECLASSIFIED
 Authority E.O. 13526
 By SP8 NARA Date 10/4/11

TOP SECRET "U"

-6-

TICOM/I-191

by piecing together the various cypher elements, more and more repeats come to light and in the case of letter text we can gradually recognise word structure, e.g. repetition of the same cypher element at definite intervals. This work is as if we were clearing away the poly equivalence from the messages. It shows as follows in our frequency counts. If the pages of the code have more than one number each, we can, after having entered the A position in rows, combine these rows; we then speak of an "overlap". Thus if in a 10 x 10 square the cypher elements have been entered according to page encyphernment I (see page 2) the rows can then be combined;

	0	1	2	3	4	5	6	7	8	9
0										
1										
2										
3										
4										
5										
6										
7										
8										
9										

Having investigated the messages for repeats and word structure, we proceed to try to break in at these points.

If passages showing structure occur at the beginning or end of a message, they may be assumed to be addresses or signatures, i.e. proper names. These are often also given in P/L messages from the network concerned

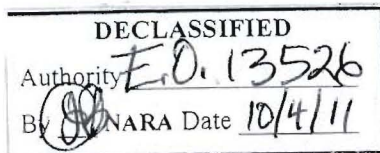
but we also try to learn names from the evaluation section.

Another point of attack in letter text are the place names which may be suspected in messages with co-ordinates. Of course one must previously have ascertained in which area the traffic lies.

Soon we shall also be able to distinguish figure text. This will be shown by frequent double or triple recurrences. If we can then tentatively identify the figures with our own or enemy units we shall endeavour to establish them, as even to recover the figures only of a code is of great value, enabling us to establish newly appearing units in a definite area. Therefore all passages with suspected figure text are written out and examined for structure. If two and three place groups for enemy units in this area occur and have the same figures, reconstruction is possible. The encyphered date and the time of day at the beginning of the message are also of use. On one occasion I reconstructed the figures of a code by means of the date and the enumeration of calibres of German A.A.

At the same time efforts are made to ascertain the indicators "read words", "read figures" and "read letters" and also the punctuation marks (.), (,), (-) etc. By these means one can fix the beginning and ending of sentences which is naturally a great help.

Simultaneously the reconstruction of the words is proceeding and therewith penetration of the code text. This work too must be done in close collaboration with the evaluation from whom the cryptanalyst may learn the type of network, whether artillery code or Ic code etc.

TOP SECRET "U"

-7-

TICOM/I-191

Attention is directed primarily to the message beginning and end, for here date, address and signature are probably to be found. If for example a cypher element almost always occurs only at the beginning or end of a message it may be suspected to be a rank or appointment; e.g. НАЧ. ШТАБА (= chief of staff). Also one may look for units such as ДИВИЗИЯ (division), ПОЛК (regiment), АРМИЯ etc. I once solved a Ic-code from the beginning by assuming that a Ic message would probably begin with ПРОТИВНИК (the enemy), this proving correct.

The cypher elements following suspected figure text are also examined; they may again be unit designations, arms, "P/W's"; the insertion of such words is relatively easy once the figure code has been partially recovered. ЧАСОВ (time) also frequently follows figures.

Another point of attack is the P/L passages frequently inserted by the Russians in 3/F messages. They often gave word and names not contained in the code in P/L. It was then easy to recover the cypher elements immediately preceding and following. All this work is naturally only possible by constantly comparing messages with each other. An experienced cryptanalyst must have the frequent cypher elements in his head and always be ready to accept new hypotheses and reject old ones.

A special class of messages is those with grid references. Having ascertained from the evaluation whether they concern the line of the front or rear areas, in which case they might be locations of HQ's or similar points, or whether they are references in front of the line which might be targets for attack, we can then attempt to insert identifications from the map. One would expect points of the compass and also geographical terms such as "forest", "coppice", "strip", "area" and military terms such as "sector" etc., to occur.

Work on short messages will be described for the И-3 system, and can be used here also.

Words which have been found must then correspond as far as possible with the position of the letters ascertained in the 10 x 10 square. If for example a cypher element has been identified as "СООБЩИТЕ" and its neighbours in the square are elements beginning with Д, the newly identified word must then not be "СООБЩИТЕ" (report) but "ДОЛОЖИТЕ" (submit).

3/F systems were always solved when sufficient material on one encypherment was available.

DECLASSIFIED	
Authority	E.O. 13526
By	NARA Date 10/4/11

TOP SECRET "U"

-8-

TICOM/I-1914/F systems

These were used from corps to army and from army to army group. For this reason they were of especial importance and great value was attached to their solution. I can no longer remember these codes in detail. I know that I have worked on the R 4Z C1800 but no longer have any clear idea of it. I will therefore as before record my experience in the hope that it may be of some use.

Before one can proceed to solve a code, one must first aim at obtaining a large amount of similar material, e.g. messages on the same recypherment. A large amount of material is therefore absolutely necessary, and the majority of unsolved 4/F codes were abandoned because of an insufficient number of messages. A more frequent change of recypherment would have made decypherment impossible.

This similar material was then subjected to frequency counts. In doing this similar cypher elements could be picked out and important repeats established, and in certain circumstances one could find the first evidences of word structure in this way. The 4/F codes had almost without exception block numbering, in the BC positions or in the AB and BC positions. This block numbering or poly-equivalence could be ascertained by means of the repeats. Thereby the "blocks" were discovered and when these had been only partially recovered one could find further repeats and word structure, in the case of letter text.

One then tried to break into this letter text, but naturally one could not take advantage of common words such as HEMEDIJEHHO or OBCPOHA with their well-known structure, for these words were given their own cypher elements in the code. It was very common for the structure of the ends of messages to be worked on, as here or at the beginning of the message one expected to find proper names. These were frequently sent in F/I and were then listed to find out at which units or HQ's the persons mentioned were. The evaluation section often supplied us with names.

One also tried to insert place names, particularly in the case of transport or supply codes. We possessed for example several messages on a traffic established by T.A. as a supply traffic, in which truck numbers were given in clear. Between these truck numbers were cypher elements with obvious structure. As the area in which the code was used was also known, and the cypher passages were assumed to be place names, possible names e.g. those lying on the supply routes were sought. By inserting them a tentative letter text was obtained, the likelihood of which could then be checked by other messages. Another point of attack, again with numbers, were messages in which numbers of our own or of enemy formations were mentioned. Even if the rest of the code had not yet been solved, the insertion of numbers often gave useful results, when previously unknown enemy units could be established thereby.

DECLASSIFIED
 Authority E.O. 13526
 By SP8 NARA Date 10/4/11

TOP SECRET "U"

-9-

TICOM/I-191

We should mention however that in the codes for individual units (e.g. 26th rifle division = 3409) separate cypher elements were provided; but owing to careless encyphering the various units were often sent with every simple number encyphered [in full]. One could then break in. And when mentioning enemy units the encypherer was naturally forced to encypher each number separately. In one code I once recovered the numbers by means of a message in which the number and calibre of guns in German A.A. units were given.

In connection with letter text, the Russian often spelt with the first two letters of the words occurring in the code. For example if he wished to send **HEMCCF** he could take after the indicator "read letters":

HE - from HEМЕДЛЕННО,
 MC - from ИСПОЛНЕНИЕ, and so on.

The word text was recovered simultaneously with the letter and figure text, each depending on the other. It was important to solve the messages as completely as possible. Recovery of words was much easier when in addition to the indicators the punctuation signs had been recovered, and when one knew which cypher elements represented figures, or one had perhaps already recovered the letter text.

Here again beginning and end were scrutinised, as containing address or signature. A cypher element occurring almost always in these two positions might be a rank or appointment, e.g. НАЧ. ШТАБА (chief of staff) or НАЧ ОПЕРОТДЕЛА (chief of operational section).

Following figure text units, arms, P/W's etc., could be guessed. Here one naturally cannot give a theoretical "unfailing" method of breaking. What is correct in one instance may be false in another. Thorough knowledge of the material and instinct are the most important factors.

It is usual to obtain the first word identifications from the short messages of 2 or 3 cypher elements. These are routine orders from a superior authority:

ДОЛОЖИТЕ ОБСТАНОВКУ = report situation,
 СРОЧНО ДОЛОЖИТЕ ОБСТАНОВКУ = report situation immediately.

The short message from the subordinate unit might then be identified as: ОБСТАНОВКА БЕЗ ИЗМЕНЕНИЙ
 = situation unchanged.

These identifications were then inserted in all messages where they occurred, affording the first steps towards solution; they could often be added to if favourable passages of P/L were interspersed. Messages with grid references, giving the front line or HQ locations, are also useful. Here close collaboration with the evaluation section is absolutely necessary. With luck words such as "river", "wood", prepositions and points of the compass may be inserted.

If one has got so far, the code may be considered partially broken. Given sufficient messages new identifications will always become evident.

DECLASSIFIED
 Authority E.O. 13526
 By SP8 NARA Date 10/4/11

TOP SECRET "U"

-10-

TICOM/I-191

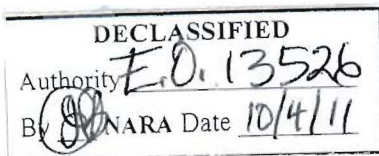
Transposition systems

These were comparatively rarely used by the Russians, who were usually content with substitution systems, e.g. substitution alphabets and codes.

I do not know whether such transposition systems were solved at Sigint Stn. 1, however I know that transposition messages were being read, that "stencils" etc., were used; however I think they were solved at General of Sigint's. The following remarks are not based on my personal experience but on the course which I attended at General of Sigint's from October, 1944 - end of December, 1944. The same importance was not attached there to these types of encypherment for Russian as there was in the course for English which ran about the same time, as we were told even then that the Russians rarely used these systems, but that they were the prevailing systems in the armies of the Western powers.

The first step is to determine the key length, e.g. the number of letters which are transposed among themselves. This was done by lining up the messages; they were written out in long lines under each other and the lowest message shifted one place at a time, the number of times "clicks" were obtained being counted. With sufficient material the key length must reveal itself. Hollerith machines were available for this laborious work of comparison. The shorter the key length the easier to find. Having ascertained it, the message was written out in a cage of this length. If in the following example the length had been found to be 16 by lining up a large number of messages, the message was written out in a cage of 16 and the lines then retransposed until with luck and patience a break in was found. For this figure text, names, message beginnings and endings etc., were helpful as before. Thus looking at the message given in Appendix "A" the figures in the first group attract our attention. Being at the beginning they can be assumed to be a date. If we know that the message was sent on 13/12/44, we can tentatively insert the date. This leaves the elements Д, Г, Н, Я, В, (.) over in the first line. It is fairly easy to reconstruct the message beginning as follows: "ДНЯ 13 (.) 12 (.) 1944 Г (.)" and the message is thus solved, as with the help of the second line the key is quickly arrived at: 3, 8, 10, 16, 6, 12, 13, 15, 1, 7, 9, 14, 2, 4, 5, 11. The solved message will then read:

ДНЯ 13 . 12 . 1944 Г . в 07 часов -- пошел - в -
 плен - немецкий - сержант - разведывательного -
 отдела . Я - его - сейчас - отослал - с двумя
 - солдатами - к - штабу - дивизии . Против-
 ник потерял - 6 - офицеров - 37 - солдат ,
 1 - противотанковое - орудие - 2 - коро -
 бочки , 5 - пулеметов - и - 30 - ружей .
 Начальник - штаба полка Попов



TOP SECRET "U"

-11-

TICOM/I-191

Translation: "on 13/12/44 at 07 hours a German sergeant of the recce detachment was taken prisoner. I sent him to div. HQ at once with 2 soldiers. The enemy lost 6 officers, 37 soldiers, 1 A/T gun, 2 tanks, 5 m.g.'s and 30 rifles. Chief of Regt. Staff Popoff".

The transposition key was obtained from a square 4×4 ($= 16$) with a stencil of the form shown, which was successively rotated 90° clockwise, the figures being read from left to right and top to bottom.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

In conclusion I repeat that I have had no practical experience of transposition systems at Sigint Stn. 1, but have based the above description on the cryptanalysis course. I will therefore give a short description, to show what training a cryptanalyst was normally given.

Cryptanalysis course

In August 1944 an examining board arrived at the Russian interpreters' company and gave the higher classes in the interpreters' training school a series of intelligence tests, Russian word puzzles and numerical puzzles were set, these being successfully solved by 12 out of the 150 - 200 persons tested. These were sent at the beginning of October to Jüterbog to the so-called cryptanalysis course. Oberfunker Wein, sometime lecturer in philosophy at Berlin University, conducted the course under the supervision of Oberinsp. Kühn.

We began with simple substitution in German and in general most systems were first treated in German and then in Russian. Then followed in logical sequence:

- substitution with more than one equivalent,
- substitution with alternative significations [mehrdentig] (indicators,)
- syllabic substitution,
- P.T. 39,
- the other substitutions in 10×10 tables introduced by the Russians during 1941/42,
- 3/F codes, 4/F codes,
- columnar substitution,
- periodic substitution [Springcäsaren],
- introduction to transposition systems.

The course was based in part on actual Russian messages but these, and also the systems, were out of date, so that though the course afforded the groundwork, one had no opportunity until arriving at Sigint Stn. 1 of becoming familiar with the more up-to-date material. Obviously as one requires a large amount of message material in the case of actual codes, the big codes were not illustrated in this way by practical examples during the course, although in practice the majority of cryptanalysts were working on such 4/F codes.

Dr. Wilhelm Gerlich.

[Trans: A.C.J.] $\frac{1}{2}$

DECLASSIFIED
 Authority E.O. 13526
 By [Signature] NARA Date 10/4/11

TOP SECRET "U"

-12-

TICOM/I-191

APPENDIX "A"

.ЧДГ .31Н 9ЯВ. 1421 ПЛО- ВСО7 ПЧ-О
 ВА-А ЕЙП- С-ЦЛ КЕЕН ЕИМН ЗЫРВ АТВЖ
 ЕАТ- РДАН ОЛЕА .ОТЛ ДЬЯГ ОЕ-Н АТ-О
 СССЕ -ГЛЕ ЙОЧО ЯЛАД АД-Л С-ТВ УОМС
 АДАИ ВКБМ УИИ- Ш-Т- ИКЗ- ППВИ НИОР
 ОИТ- ОБТР ОЛФЕ ИРВ- БЦ-Я А--Л РСТЗ
 ,700 ЛИД- О-ТО РТВИ ОВУА НЕКО РЧДК
 И2ОИ БЕ,- КОО- ТИ5- ЕЛО- ВПОЕ М-ЕУ
 АВ-Н ИЕЧР АЖКЙ .ЛН-П ОБКШ АТВА
 ППОА

The message is written out in the key length:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Number of column
.	ч	д	г	.	з	1	н	9	я	в	.	1	4	2	1	
п	л	о	-	в	с	о	7	п	ч	-	о	з	а	-	а	
е	й	п	-	с	-	ц	л	к	е	о	н	е	и	м	н	
з	ы	р	в	а	т	в	ж	е	а	т	-	р	д	а	н	
о	л	е	а	.	о	т	л	д	ь	я	г	о	е	-	н	
а	т	-	о	с	с	с	е	-	г	л	е	й	о	ч	о	
я	л	а	д	а	д	-	л	с	-	т	в	у	о	м	с	
а	д	а	и	в	к	б	м	у	и	и	-	ш	-	т	-	
и	к	з	-	п	п	в	и	н	и	о	р	о	и	т	-	
о	е	т	р	о	л	ф	е	и	р	в	-	б	ц	-	я	
а	-	-	п	р	с	т	з	,	7	о	о	л	1	д	-	
о	-	т	о	р	т	в	и	о	в	у	а	н	е	к	о	
р	ч	д	к	и	2	о	и	б	е	,	-	к	о	-		
т	и	5	-	з	л	о	-	з	п	с	е	м	-	е	у	
а	б	-	н	и	е	ч	р	а	у	к	й	.	л	н	ж	
л	о	-	п	о	б	к	ш	а	т	в	а	п	п	о	а	